جامعة بيرزيت

BIRZEIT UNIVERSITY

Secure Software Development (SWEN7302)
Dr: Ahmad Alsadeh

Homework Assignment # 1

By Hanan Namrouti(1165217)

1. Why is waiting to think about security until after the software is built a bad idea?

Definitely its bad idea, thinking of security requirement from the beginning is less expensive , fixing problems later is more complex, moreover sometimes to include security later stages require redesign which may cause problems and bugs in more than one components .

2. What is an abuse case?

- **A scenario that illustrates a potential failure in security under relevant circumstances**

Abuse case is a use case from an attacker perspective with the intent to harm the system, A misuse case is the inverse of a use case, i.e., a function that the system should not allow. Just as defines a use case as a completed sequence of actions which gives increased value to the user, one could define a misuse case as a completed sequence of actions which results in loss for the organization or some specific stakeholder.[1]

3. What is a reason for making an explicit threat model when designing a system?

- So that you avoid an incoherent defense
- So you can defend against the most likely/costly/important attacks
- So you can explicitly list and challenge assumptions that underlie your design

4. Suppose you design software for a bank and the bank's customers may remotely log into its site using commodity PCs. These PCs might have malware on them, which could log keystrokes or read files stored on the machine. Which threat model makes the most sense for you to consider, when designing the bank's site?
User level model

5. What is a good defense against powers that are particular to a snooping user?

- Using encryption: Snooping users can view the network message traffic of others interacting with a site, so encrypting that traffic limits the negative effects of snooping

6. A denial of service attack violates what security policy/goal?

- Availability

7. When talking about computer security, what do we mean by the term, principal?

[1] "Capturing Security Requirements through Misuse Cases." http://hjem.ifi.uio.no/nik/2001/21-sindre.pdf. Accessed 29 Nov. 2017.

- An actor, or role, that is the subject of a security policy: Principals can be people, computer programs, or some other entity acting in a particular role, like *manager* or *client*

8.Passwords, biometrics, and user-owned SMS-receiving mobile phones are useful for what security mechanism?

- Authentication

9.We identified three categories of secure design principles: prevention, mitigation, and recovery. Running each browser tab in a separate OS process (as done by the Chrome browser) is an example design illustrating which category?

Recovery: You could argue that isolating a tab makes it easier to recover from a breach

10. Suppose you are implementing a graphical user interface for using a library implementing the RSA cryptosystem, and you want to give users a way to generate new keys. How do you do that taking security designs into account?

Allow the user to use a slider to choose the number of bits, setting slider initially to point at 2048 bits. As the user moves the slider to larger or smaller values, visualize the difference in relative protective power, e.g., using a meter

11. Suppose you are implementing an extensible data management system. You want to accommodate plug-ins that can implement storage rules and query processing functionality for different data formats (e.g., relational data, object data, XML data, etc.). How do you do that considering the security designs?

- The plug-ins are implemented as separate OS processes; these processes communicate to/from the main process to handle queries/updates for the data formats they support

12. Promoting privacy is a goal that follows from which category of secure design principle?

- It is an example of trusting with reluctance because promoting privacy means sharing private information with as few software components as possible, meaning that fewer need to be trusted to protect the information

13. Encrypting a password database is an example of what category of design principle?

- It is an example of *defense in depth*

14. Which of the following vulnerabilities can VSFTPD's secure string library help protect against?

- Integer overflow
- Buffer overflow

ndle each client connection. It could have, instead, spawned a thread within the main process to handle each connection, as is done in many servers. How would this alternative design compare to the original?

- It would be less secure because a compromise by a malicious client in one thread could (more easily) access data used by another client's thread, since they share the same address space

16. FTP servers can be asked to list a directory of files. VSFTPD could do this by calling the system's ls (or dir) command, displaying the result to a client. But VSFTPD does not do this, and implements directory listings using the relevant system calls directly. Why might you argue that VSFTPD's design makes sense from a security perspective

ls does more than is needed, and thus unnecessarily expands the TCB
Calling ls involves forking a new process, which is less secure than running within the same process
Calling ls doesn't give us any way to employ fail-safe defaults
Using ls provides less control over the output, which leaves users open to XSS-style attacks